ERROR-CORRECTING CODES

SECOND EDITION

W. WESLEY PETERSON
E. J. WELDON, JR.

LAND

Eighth printing, 1986

Set in Monotype Times New Roman
Printed by Halliday Lithograph Corporation.
Bound in the United States of America by Halliday Lithograph Corporation.

Sixth printing, July 1981

ISBN 0 262 16 039 0 (hardcover)
Library of Congress catalog card number: 76-122262

8.2 Matrix Description of Cyclic Codes

The most elementary description by matrices has been illustrated in the previous section. If $g(X) = a_r X^r + a_{r-1} X^{r-1} + \cdots + a_0$ is the generator of the code, then $\{X^{n-r-1}g(X)\}, \{X^{n-r-2}g(X)\}, \ldots, \{g(X)\}$ are all code vectors. Thus, all the rows of the following matrix are code vectors:

$$\mathbf{G} = \begin{bmatrix} a_r & a_{r-1} & \cdots & a_0 & 0 & & 0 \\ 0 & a_r & a_{r-1} & \cdots & a_0 & 0 & 0 \\ \vdots & & & & & & \\ 0 & 0 & & a_r & a_{r-1} & \cdots & a_0 \; 0 \\ 0 & 0 & & 0 & a_r & \cdots & a_0 \end{bmatrix} \tag{8.3}$$

Clearly, they are linearly independent, and the rank of $\mathbf{G}$ is $n - r$, which is also the dimension of the code. Therefore, by Theorem 2.9 the row space of $\mathbf{G}$ is the code space.

As earlier, the following convention will be used. The first k symbols, coefficients of X^{n-1}, X^{n-2}, ..., X^{n-k}, will be taken as information symbols, and the last $n - k$ symbols, coefficients of X^{n-k-1}, X^{n-k-2}, ... 1, will be taken as parity-check symbols.

The generator matrix for any cyclic code can be put in modified reduced echelon form as follows. Let $r_i(X)$ be the remainder after dividing X^i by $g(X)$:

$$X^i = g(X)\, q_i(X) + r_i(X).$$

Then

$$X^i - r_i(X) = g(X)\, q_i(X)$$

is a code vector. If these polynomials, for $i = n - 1, n - 2, \ldots, n - k$, are taken as rows of the generator matrix, then

$$\mathbf{G} = [\mathbb{I}_k, -\mathbb{R}],$$

where $\mathbb{I}_k$ is a $k \times k$ identity matrix and $-\mathbb{R}$ is a $k \times (n - k)$ matrix whose jth row is the vector of coefficients of $-r_{n-j}(X)$. Then by Theorem 3.3 the code is also the null space of the matrix

$$\mathbb{H} = [\mathbb{R}^T, \mathbb{I}_{n-k}].$$

The jth row of $\mathbb{H}^T$ is the vector of coefficients of $r_{n-j}(X)$, *even for* $j \leqq n - k$.

Example. For the binary cyclic code generated by $f(X) = X^3 + X^2 + 1$,

$$\begin{array}{lll} X^6 = g(X)(X^3 + X^2 + X) + X^2 + X & & \\ X^5 = g(X)(X^2 + X + 1) \quad\quad + X + 1 & & \\ X^4 = g(X)(X + 1) \quad\quad + X^2 + X + 1 & & \\ X^3 = g(X)(1) \quad\quad + X^2 \quad\quad + 1 & \mathbf{H}_1^T = & \begin{bmatrix} 1\,1\,0 \\ 0\,1\,1 \\ 1\,1\,1 \\ 1\,0\,1 \\ 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix} \\ X^2 = g(X)(0) \quad\quad + X^2 & & \\ X^1 = g(X)(0) \quad\quad + X & & \\ X^0 = g(X)(0) \quad\quad + 1 & & \end{array} \tag{8.4}$$

and

$$\mathbf{G}_1 = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1\,1 \\ 0\,0\,0\,1\,1\,0\,1 \end{bmatrix} \tag{8.5}$$

The matrix **G** given here is row equivalent to the matrix given in Equation 8.1. The code is the same code, not just an equivalent code.

Now consider the dual code that, by Theorem 6.12, is generated by $(X^7 - 1)/g(X) = (X - 1)(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$:

$$\begin{array}{lll} r_6(X) = X^3 + X^2 + X & & \\ r_5(X) = \quad X^2 + X + 1 & & \\ r_4(X) = X^3 + X^2 \quad\quad + 1 & & \\ r_3(X) = X^3 & \mathbf{H}_2^T = & \begin{bmatrix} 1\,1\,1\,0 \\ 0\,1\,1\,1 \\ 1\,1\,0\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{bmatrix} \\ r_2(X) = \quad X^2 & & \\ r_1(X) = \quad\quad X & & \\ r_0(X) = \quad\quad\quad 1 & & \end{array} \tag{8.6}$$

and

$$\mathbf{G}_2 = \begin{bmatrix} 1\,0\,0\,1\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1\,1 \\ 0\,0\,1\,1\,1\,0\,1 \end{bmatrix} \tag{8.7}$$

The matrices $\mathbf{H}_1$ and $\mathbf{G}_2$ differ in having the order of columns reversed and the rows reversed, and the same is true of $\mathbf{G}_1$ and $\mathbf{H}_2$. The rearrangement of rows does not affect the row space or null space. The rearrangement of columns is a result of the fact that two polynomials multiply to zero only if the dot product of the vectors, with the order of components reversed in one of them, is zero.

and by Theorem 6.14, its conjugates are cyclic shifts of this polynomial; that is,

$$\beta^2 = \alpha^{27} + \alpha^{26} + \alpha^{25} + \alpha^{24} + 0 + \alpha^{22} + 0 + 0,$$
$$\vdots$$
$$\beta^{27} = \beta^9 = 0 + 0 + \alpha^{25} + \alpha^{24} + \alpha^{23} + \alpha^{22} + \alpha^{21} + \alpha^{20}.$$

With some effort it can be shown that $\beta^3 = \alpha^{25} + \alpha^{20}$. Then the conjugates of β^3 consist of cyclic shifts of the 8-tuple 00100001. The root β^0 can be shown to equal $\alpha^{27} + \alpha^{26} + \alpha^{25} + \alpha^{24} + \alpha^{23} + \alpha^{22} + \alpha^{21} + \alpha^{20}$. (See Problem 8.23.) Thus, the matrix $\mathbf{H}$ can be rearranged to give

$$\mathbf{H} = [[\beta^9\beta^{13}\beta^{15}\beta^{16}\beta^8\beta^4\beta^2\beta^1][\beta^{10}\beta^5\beta^{11}\beta^{14}\beta^7\beta^{12}\beta^6\beta^3]\beta^0]$$

$$= \left[\begin{bmatrix}0\,1\,0\,1\,1\,1\,1\,0\\0\,0\,1\,0\,1\,1\,1\,1\\1\,0\,0\,1\,0\,1\,1\,1\\1\,1\,0\,0\,1\,0\,1\,1\\1\,1\,1\,0\,0\,1\,0\,1\\1\,1\,1\,1\,0\,0\,1\,0\\0\,1\,1\,1\,1\,0\,0\,1\\1\,0\,1\,1\,1\,1\,0\,0\end{bmatrix}\begin{bmatrix}1\,0\,0\,0\,0\,1\,0\,0\\0\,1\,0\,0\,0\,0\,1\,0\\0\,0\,1\,0\,0\,0\,0\,1\\1\,0\,0\,1\,0\,0\,0\,0\\0\,1\,0\,0\,1\,0\,0\,0\\0\,0\,1\,0\,0\,1\,0\,0\\0\,0\,0\,1\,0\,0\,1\,0\\0\,0\,0\,0\,1\,0\,0\,1\end{bmatrix}\begin{matrix}1\\1\\1\\1\\1\\1\\1\\1\end{matrix}\right] = [\mathbf{C}_1\mathbf{C}_2].$$

Therefore, the (17, 9) code with one information symbol deleted is equivalent to a (16, 8) quasi-cyclic code. Because $\mathbf{C}_2$ is nonsingular, the matrix $[\mathbf{C}_1\,\mathbf{C}_2]$ can be put in echelon canonical form by multiplying it on the left by the inverse of $\mathbf{C}_1$.

It is known that every finite field has a normal basis (Albert 1956, p. 119). Thus, the generator matrix of every cyclic code can be decomposed into circulants, although many will be trivial. Then, removing columns corresponding to elements of order less than n will give the generator matrix of a quasi-cyclic code. It may not be possible to put such a code in systematic form, however.

8.15 Codes Based on the Chinese Remainder Theorem

Let $i(X)$ denote a polynomial of degree $k-1$ or less with symbols from $GF(q^m)$. Let $m_i(X)$ denote a polynomial of degree d_i with symbols from the same field. An interesting class of codes can be constructed from the following version of the Chinese Remainder Theorem (Stone 1963).

THEOREM 8.20. *The polynomial $i(X)$ can be reconstructed from the remainders*

$$r_i(X) \equiv i(X) \bmod m_i(X) \qquad i = 1, 2, \ldots, n, \tag{8.56}$$

provided the $m_i(X)$ are relatively prime in pairs and that

$$\sum_{i=1}^{n} d_i > k - 1. \tag{8.57}$$

Proof. Any two solutions $i_1(X)$ and $i_2(X)$ to the set of congruences (8-56) are congruent modulo $m(X) = \prod_{i=1}^{n} m_i(X)$; for $i_1(X) - i_2(X)$ is divisible by $m(X)$ if and only if it is divisible by each $m_i(X)$. Since there is exactly one polynomial of degree less than k in each residue class modulo $m(X)$, there is exactly one solution for the set of congruences (8.56), and this must be the correct solution. Q.E.D.

This theorem can be used to construct a class of random-error-correcting codes with symbols from $GF(q^m)$ as follows: Choose as the $m_i(X)$ the factors of $X^{q^m-1} - 1$ in $GF(q^m)$. Since this polynomial splits completely in $GF(q^m)$,

$$m_i(X) = (X - \alpha^i), \qquad i = 0, 1, \ldots, q^m - 2,$$

where α is a primitive element of $GF(q^m)$.

Now calculate the $n = q^m - 1$ residues of the information polynomial $i(X)$ which has degree less than k. The set of these polynomials forms an (n, k) linear code with symbols from $GF(q^m)$.

Decoding can be performed as follows: Suppose t errors occur so that $n - t$ of the residues are received correctly. Now, $i(X)$ is determined by any set of k correct residues. Thus, of the $\binom{n}{k}$ ways of determining $i(X)$, exactly $\binom{n-t}{k}$ will agree and give the correct polynomial $i(X)$. It is possible that $t - 1$ transmitted residues have been changed so as to be the residues of some other polynomial $j(X)$ of degree $k - 1$ or less which is determined by $k - 1$ correct residues and one incorrect residue. There are

$$\binom{k-1+t}{k}$$

determinations which will give the same incorrect answer.

Now if $n - t > k - 1 + t$, then the number of correct determinations exceeds the number of incorrect ones, so $i(X)$ can be reconstructed correctly. That is, if t is chosen such that

$$2t + 1 = n - k + 1$$

for a particular code, then all t errors can be corrected. Since the minimum distance is not less than $2t + 1$, and since $d \leqq n - k + 1$ for any linear code, it follows that for these codes,

$$d = n - k + 1.$$

It turns out that these codes can be put in a cyclic form. The residue of $i(X) = i_{k-1}X^{k-1} + i_{k-2}X^{k-2} + \cdots + i_1X + i_0 \bmod (X - \alpha^i)$, which is an element of $GF(q^m)$, is given by

$$i(X) = r_i + g_i(X)(X - \alpha^i).$$

Thus

$$r_i = i(X)|_{x=\alpha^i} = i(\alpha^i).$$

Let the generator matrix of an (n, k) code with symbols in $GF(q^m)$ be

$$\mathbf{G} = \begin{bmatrix} (\alpha^{k-1})^{n-1} & (\alpha^{k-1})^{n-2} & \cdots & \alpha^{k-1} & \alpha^0 \\ (\alpha^{k-2})^{n-1} & (\alpha^{k-2})^{n-2} & \cdots & \alpha^{k-2} & \alpha^0 \\ \vdots & & \cdots & & \vdots \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^1 & \alpha^0 \end{bmatrix} \tag{8.58}$$

Multiplying $\mathbf{G}$ by the information vector $= (i_{k-1}i_{k-2}\cdots i_0)$ gives the n-tuple

$$[i(X)|_{X=\alpha^{n-1}}, i(X)|_{X=\alpha^{n-2}}, \ldots, i(X)|_{X=\alpha}, i(X)|_{X=1}] = [r_{n-1}, r_{n-2}, \ldots, r_1, r_0], \tag{8.59}$$

which is a code word in the code based on the Chinese Remainder Theorem.

But $\mathbf{G}$ is the generator matrix of the cyclic (n, k) code for which $h(X)$ has roots $\alpha^1, \alpha^2, \ldots, \alpha^{k-1}$. In fact, this is a Reed-Solomon code and is discussed at length in the next chapter.

The decoding procedure presented here for these codes is clearly impractical for all but the shortest codes. It requires that the decoder perform $\binom{n}{k}$ operations for each decoding. Fortunately a more easily mechanized method of decoding these very powerful codes has been found; it too is discussed in Chapter 9.

Since a symbol in $GF(q^m)$ can be represented as an m-tuple over $GF(q)$, these codes are ideally suited to multiple burst-error correction. This is discussed in Chapter 11.

It is not necessary to consider linear factors in an extension field; polynomials of higher degree over $GF(q)$ also yield interesting codes.

Solomon codes and interleaved Reed-Solomon codes, have good burst-correcting capabilities. In particular, a Reed-Solomon single-error correcting code over $GF(q^b)$ interleaved to degree i has exactly the same parameters and burst-correcting capability as the block-interleaved Burton code (Equation 11.7) with $n' = q^m - 1$, the maximum possible value. (See Problem 11.10.) Note that as a code over $GF(q^m)$ the t-error correcting Reed-Solomon code requires $2t$ check symbols and corrects, among other patterns, every burst of length t or less. Thus every Reed-Solomon code, as a code over $GF(q^m)$, is optimal with respect to the Reiger bound. It follows, as for the Burton codes, that as codes over $GF(q^m)$ they are asymptotically optimal. The multiple-burst-error correcting capability of such codes is discussed in Section 11.4.

Example. A Reed-Solomon code with symbols from $GF(2^7)$ and $t = 4$ could be used to correct all bursts of length 22 or less by coding symbols as blocks of 7 binary digits. It would require $2 \times 4 = 8$ blocks or $8 \times 7 = 56$ binary symbols as parity checks. The code length would be $7 \times (2^7 - 1) = 889$.

A Fire code to correct all bursts of length 22 or less would require $3b - 1 = 65$ binary digits as parity checks. The code length could be as great as $(2^{22} - 1) \times 43$, or approximately 160 million binary digits. On the other hand, a burst of length 8 binary digits or less could affect at most two elements of $GF(2^7)$, and thus the Reed-Solomon code could correct any two bursts of length 8 or less. It could correct as many as four bursts if each happened to lie within a single $GF(2^7)$ element.

From Equation 11.7, there exists a (3556, 3500) Burton code with $b = 22$ and $z = 12$. Note that this code has the same burst-correcting ability and number of parity checks as the Reed-Solomon code but is four times longer. It cannot correct multiple bursts, however.

BCH codes can be implemented by the methods described in Chapter 9. Alternatively, if correction of single bursts only is sufficient, the method of Section 11.3 can be used, and requires much less equipment. The additional error-correcting ability of the code can be turned to error detection (any error pattern that the code would correct, if fully utilized, it could certainly still detect) or it can be used to correct bursts beyond its guaranteed burst-correcting ability. (See Section 11.3.)

THEOREM 11.4. *If a code with minimum distance d is used to correct multiple bursts of errors, then the set of all burst patterns satisfying*

$$l + P \leq \frac{3d}{4} - 1 \tag{11.8}$$